United Nations A/C.2/64/L.8

General Assembly

Distr.: Limited
22 October 2009

Original: English

Sixty-fourth session
Second Committee
Agenda item 55 (e)
Globalization and interdependence: science and technology for development

Australia, Canada, Israel, Japan, Marshall Islands and the United States of America: draft resolution

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

The General Assembly,

Recalling its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of information technologies, 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity and 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures,

Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007 and 63/37 of 2 December 2008 on developments in the field of information and telecommunications in the context of international security,

Recalling further the outcomes of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November (second phase),[1] in which States recognized that freedom of expression and the free flow of information, ideas, and knowledge are essential for today's information society and beneficial to development, and that, because confidence and security in the use of information and communications technologies are among the main pillars of the information society, a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented,

Recognizing the increasingly indispensable contribution made by networked information technologies to most of the essential functions of daily life, commerce

[1] See A/C.2/59/3 and A/60/687.

09-57346 (E) 261009

Please recycle

and the provision of goods and services, research, innovation and entrepreneurship, and to the free flow of information among individuals, organizations and Governments,

Noting that Governments, businesses, civil society and individuals are increasingly reliant upon a global network of information infrastructures, and that such reliance will only increase,

Noting also that gaps in access to and the use of information technologies by States can diminish their social and economic prosperity, and noting especially the needs of less developed countries in the areas of cybersecurity best practices and training,

Expressing concern that threats to the reliable functioning of critical information infrastructures and to the integrity of the information carried over those networks are growing in both sophistication and gravity, affecting domestic, national and international welfare,

Affirming that the security of critical information infrastructures is a responsibility Governments must address systematically and an area in which they must lead nationally, in coordination with relevant stakeholders, who in turn must be aware of relevant risks, preventive measures and effective responses in a manner appropriate to their respective roles,

Recognizing that national efforts should be supported by national, regional and international information-sharing and collaboration, so as to confront effectively the increasingly transnational nature of such threats,

Noting the work of relevant regional and international organizations on enhancing cybersecurity, especially those that have encouraged national efforts and have fostered international cooperation,

Noting also the 2009 report of the International Telecommunication Union entitled "Securing information and communication networks: best practices for developing a culture of cybersecurity", which focused on a comprehensive national approach to cybersecurity consistent with free speech, the free flow of information and due process of law,

Recognizing that national efforts to protect critical information infrastructures benefit from a periodic assessment of their progress,

1. *Invites* Member States to provide, on a voluntary basis, summaries of their key initiatives on cybersecurity and the protection of critical information infrastructures, so as to highlight national achievements and best practices, lessons learned and areas for further action;

2. *Offers* Members States, in this regard, the attached national cybersecurity self-assessment survey as a possible tool to aid them, where appropriate, in reviewing national efforts on cybersecurity and the protection of critical information infrastructures;

3. *Invites* all Member States that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to inform the Secretary-General, by the sixty-fifth session of the General Assembly, of best practices and measures that could assist other Member States, regional and international organizations, private-sector and civil society stakeholders in their efforts to create a global culture of cybersecurity.

Annex

Self-assessment tool for national efforts to protect critical information infrastructures

Taking stock of cybersecurity needs and strategies

1. Evaluate the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society.

2. Determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructures, and civil society that must be managed.

3. Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present, and the current management plan; note how changes in economic environment, national security priorities and civil society needs affect these calculations.

4. Determine the goals of your national cybersecurity and critical information infrastructure protection strategy, describe its goals, current level of implementation, measures that exist to gauge its progress, its relation to other national policy objectives, and how such a strategy fits within regional and international initiatives.

Stakeholder roles and responsibilities

5. Determine key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including:

- National Government ministries or agencies, noting primary points of contact and responsibilities of each;
- Other government (local and regional) participants;
- Non-government actors, including industry, civil society and academia;
- Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity.

Policy processes and participation

6. Identify formal and informal venues that currently exist for Government-industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and its adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.

7. Identify forums or structures that may further be needed to integrate the Government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals.

Public-private cooperation

8. Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for information-sharing and incident management.

9. Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure.

Incident management and recovery

10. Identify the agency in your Government that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information-sharing.

11. Separately, identify your national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks, and existing tools and procedures for the dissemination of incident-management information.

12. Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.

Legal frameworks

13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communication technologies, and use regional and international conventions, arrangements and precedents in these reviews. Determine whether your State is a party to, or plans to accede to the Budapest Convention on Cybercrime, or plans to adopt commensurate laws.

14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

16. Examine whether your State participates in international efforts to combat cybercrime, such as the 24/7 Cybercrime Point of Contact Network, and determine to what extent doing so would further national cybersecurity goals.

17. Determine the requirements for your national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in your national territory, but victims reside elsewhere.

Developing a global culture of cybersecurity

18. Summarize actions taken and plans to develop a national culture of cybersecurity referred to in United Nations General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements.